Cybersecurity

The Road Ahead for Defense Acquisition

Steve Mills ■ *Steve Monks*

The May-June 2014 edition on *Defense AT&L* magazine included an article by Under Secretary of Defense for Acquisition, Technology, and Logistics Frank Kendall, titled "Protecting the Future," which stressed Kendall's concern about the United States' ability to maintain its technological superiority.

Maintaining that superiority is based not only on adequate funding for leaps in technology but also on honing that technology to protect the capability against cybersecurity threats. The cyber threat we face every day is one of the greatest risks to our ability in developing, delivering and sustaining our warfighting capability. It is dynamic, adaptable and resilient, with an insidious effect on the accomplishment of the mission.

Over the last two decades, our weapon systems have become more interconnected. We now are in a system-of-systems world. Those weapon systems have become more lethal with the advent of better shared situational awareness and the ability to realize the capabilities of coordinated weapon systems that are greater than the sum of the parts. We have invested greatly in this. Today our systems are the best in the world and continue to ensure our dominance on the battlefield. However, that investment has brought greater dependence and risk. The cyber threat is growing at an increasing rate, and has the potential to significantly degrade and even eliminate our advantage on the current and future battlefield. The risks to our Department of Defense (DoD) systems have reached the point

Mills *and* **Monks** *are professors of Program Management at the Defense Acquisition University's South Region in Huntsville, Alabama, where Mills also is the Region's Cyber Lead.*

where we must change our thinking about how to combat this threat and who is responsible or involved in this fight.

How vulnerable and resilient are DoD systems against the cyber threat today? Unfortunately, testing continues to show our systems to be extremely vulnerable to the cyber threat. According to a Defense Science Board (DSB) study completed in January 2013 and titled "Resilient Military Systems and the Advanced Cyber Threat," several key findings provide great insight:

- "Current DoD actions, though numerous are fragmented. Thus, DoD is not prepared to defend against this threat."
- "DoD Red Teams, using cyber-attack tools which can be downloaded from the internet, are very successful at defeating our systems."
- "With present capabilities and technology it is not possible to defend with confidence against the most sophisticated cyber-attacks."
- "It will take years for the Department to build an effective response to the cyber threat to include elements of deterrence, mission assurance and offensive cyber capabilities."

Additionally, more recent testing demonstrates our inability to significantly reduce this risk. *The Director, Operational Test and Evaluation (DOT&E) Fiscal Year (FY) 2014 Annual Report* reveals several disturbing trends:

- Operational testing still found exploitable cyber vulnerabilities that earlier technical testing could have mitigated.
- Many of the vulnerabilities found were common and easy to address including unnecessary network services or system functions as well as misconfigured, unpatched or outdated software.

Clearly, the DoD has a lot of work to do to reverse the trend. In response to these trends and the growing cyber threat, Kendall commissioned three additional DSB Task Force Studies on the following cybersecurity focus areas:

- Cyber Supply Chain—Practices to prevent parts that contain malicious defects or malware
- Cyber Deterrence—Policy, Operational, and Technological imperatives
- Cyber Defense—How to inform future investment priorities for cybersecurity

These studies will provide additional insight into how to mitigate the cyber threat. Once the findings are released, we will need the attention and support of the entire acquisition workforce and user community to meet this threat head on.

Effective cybersecurity of DoD acquisition programs is first and foremost "leader business." Few other aspects of our weapon systems possess the potential cost, schedule, performance and risk impacts of cybersecurity. Cybersecurity impacts all facets of our acquisition programs. Leaders are quickly acknowledging the importance of cybersecurity as it relates to acquisition programs but often fail to understand that successfully addressing it in their programs is more than just a funding issue. While increased funding to address cybersecurity in acquisition programs may be required, the solution set is much more. Effective cybersecurity in DoD acquisition programs involves many other aspects such as:

- Cybersecurity leadership—Top management support for program cybersecurity
- Knowledgeable workforce (including leadership) on cybersecurity principles, risks and opportunities
- Treating cybersecurity as a true design consideration versus as an afterthought and/or "unfunded mandate"

Furthermore, leaders both expect and demand that our systems operate effectively in their intended environment. Leaders are quickly realizing the enormity of the cyber threat and that we now operate in a cyber-contested environment. Cybersecurity being treated as key "leader business" is critical to the overall cybersecurity posture of our DoD acquisition programs.

A key challenge for DoD acquisition addressing the cyber threat is how do we "bake in" cybersecurity for our DoD acquisition programs vs. "bolting it on." The dominant focus of our cybersecurity efforts today is how to secure systems that are already in the inventory. To effectively integrate cybersecurity into our DoD acquisition systems, we must change our cybersecurity focus from a reactive to a proactive, "shift left" approach. The DoD acquisition enterprise has an obligation to build systems that in the future will minimize real-time cybersecurity crises that cue reactionary measures to mitigate the damage. If we stay in the reactive mode and depend on others within the DoD to address the changing threat, we ultimately will lose our crucial ability to retain the initiative and act within the enemy's decision cycle. We must execute a shift in this fight and become proactive in every way possible regarding the cyber threat. "Bolting on" cybersecurity solutions is ineffective. The DSB Study of 2013 validates this. This drives greater cost, higher risk and a non-optimal result.

Our proactive, shift left cybersecurity approach must begin with addressing the warfighter's requirement. How do we ensure that requirements documents clearly articulate the cybersecurity need? To be sure, the acquisition community and the resources that propel our work is fairly bound by vetted requirements. Just as we have an obligation of trust to deliver secure systems so too do we depend upon the requirements community to get the requirements right. The user community and the Joint Capabilities Integration and Development System (JCIDS) process are our path to ensuring we have the right requirements; it is vital that JCIDS take up the mantle for developing operationally meaningful and proactive cybersecurity effort within the DoD. Our cybersecurity focus must be continually guided by the key JCIDS documents (Initial Capabilities Document, Capability Development Document and Capability Production Document). The designs of our sys-

A key challenge for DoD acquisition addressing the cyber threat is how do we "bake in" cybersecurity for our DoD acquisition programs vs. "bolting it on."

tems are impacted by numerous considerations, which include different operating environments and possible threats posed within the air, land, sea, space and cyberspace domains. These considerations clearly help ensure our systems are both effective and suitable for the warfighter.

In an effort to better define cybersecurity requirements as they relate to our warfighting systems, the Joint Requirements Oversight Council (JROC) issued a JROC Memorandum (JROCM) on June 3, 2015, regarding cybersecurity and its relationship to the System Survivability Key Performance Parameter (KPP). This JROCM titled, *Process to Develop Cyber Survivability Endorsement to the System Survivability KPP,* asked the Services to "nominate one of their JCIDS military needs documents as use cases" for this effort. The big question is whether or not this effort generates something other than just more cybersecurity controls and/or compliance items. While critically important to achieving and maintaining "cyber hygiene," cybersecurity controls and compliance with those controls are only parts of the solution set. In the end, cybersecurity in weapon systems acquisition is primarily about operational resiliency in a cyber-contested environment. Achieving this state remains our challenge.

The next critical component of effective and proactive cybersecurity integration into our DoD programs is to treat cybersecurity as a design consideration throughout the entire acquisition life cycle. How do we ensure that cybersecurity is treated as a design consideration with the same pedigree as other critical "ilities" versus being relegated to somewhat ad hoc efforts that are considered only at test time, and sometimes after the production decision? The concept of "shift left" from both a System Security Engineering (SSE) and T&E perspective is where we must go. Shift left from an SSE and T&E perspective is all about proactively addressing cybersecurity requirements "up front and early" in the acquisition life cycle. "Our challenge is to fully integrate cybersecurity into our test processes to help programs identify risks, minimize the attack surface and reduce kill chain effects to improve resiliency." (Steven J. Hutchison, *Defense AT&L* magazine, January-February 2015). To be effective and ultimately successful, cybersecurity must be "baked in" the design of our warfighting systems.

Supporting policy and best practices for effective cybersecurity in acquisition programs is another critical component that must be present. There has been significant progress in this area. The recently released *PM Guidebook for Integrating the Cybersecurity Risk Management Framework* (RMF) into the System Acquisition Lifecycle (https://acc.dau.mil/adl/en-US/722603/file/80119/Cybersecurity%20Guidebook%20v1_0%20with%20publication%20notice.pdf) provides clear guidance on how cybersecurity is integrated into the acquisition life cycle. *The Program Manager's Guidebook* also provides two excellent examples of how the RMF is implemented across the acquisition life cycle by acquisition phase. These examples help both leaders and acquisition workforce members gain insight into application of cybersecurity principles.

A key capability for effective integration of cybersecurity into our acquisition programs is through robust T&E in support of the system engineering effort. The recently released *Cybersecurity Test and Evaluation Guidebook* dated July 1, 2015 (http://www.dote.osd.mil/docs/TempGuide3/Cybersecurity_TE_Guidebook_July1_2015_v1_0.pdf) provides clear guidelines and best practices to support ongoing and future cybersecurity T&E. This guidebook is divided into two key components. The first component provides essential information for T&E personnel on how to effectively support the RMF. The remaining component describes and addresses the implementation of cybersecurity T&E across the acquisition life cycle. Combining the T&E-related guidance provided by the cybersecurity T&E with the overarching focus of the *Program Manager's Guidebook for Integrating the Risk Management Framework* provides both leaders and acquisition workforce member's critical insight into how cybersecurity should be integrated into the DoD acquisition life cycle.

Who in the acquisition workforce needs to be involved in addressing the cyber threat? The short answer is: Just about everyone! Cybersecurity continues to remain a team sport. The threat is growing, dynamic and evolving. It is a difficult problem. Acquisition workforce members need to be both aware and proactive from a cybersecurity perspective. If this occurs, the DoD can win this fight. If everyone takes the attitude that it's someone else's issue, the DoD will remain at risk. In the past, the focus of cybersecurity (formerly called information assurance) was security of the network and was primarily a concern for Information Technology career field personnel. This is clearly no longer the case. Cybersecurity is now a concern for all career fields and applies to all DoD systems that process DoD information.

To be successful in this effort, the DoD needs the energy, critical thinking and focus of the entire acquisition community, user community and our industry partners right now. This will take time to get right, but it can and must be done. In the end, it will come down to hard work, motivated acquisition professionals in all career fields treating cybersecurity as a design consideration, and informed leaders who make cybersecurity of DoD acquisition programs a priority.

The authors can be contacted at **steve.mills@dau.mil** *and* **steve.monks@dau.mil**.